

UNITED STATES DISTRICT COURT
WESTERN DISTRICT OF NEW YORK

REDACTED VERSION

UNITED STATES OF AMERICA,

**REPORT, RECOMMENDATION
AND ORDER**

v.

21-CR-0007(LJV)(JJM)

JOHN STUART,

Defendant.

Defendant John Stuart is charged in an eight-count Indictment [8]¹ with child pornography, controlled substance, and firearm offenses. These charges arise from an October 8, 2020 search warrant issued by United States Magistrate Judge Michael J. Roemer for Stuart's residence. Stuart's initial motion to suppress the evidence derived from that search and for discovery was denied. *See* December 15, 2021 Report, Recommendation and Order [33], adopted, April 7, 2022 Decision and Order [44]. After learning more about the underlying investigation that led to the search warrant, Stuart moved for additional relief.

Currently before the court are Stuart's motion to compel [55], motion to vacate the Protective Order [85], and supplemental motion for a hearing pursuant to Franks v. Delaware, 438 U.S. 154 (1987) and suppression [89]. Having reviewed the parties' submissions [55, 66, 71, 75, 80, 85, 87-89, 92], and heard argument on January 25 and March 8, 2023 [74, 81], for the following reasons the motions to compel and vacate are denied, and I recommend that the motion for a Franks hearing and to suppress likewise be denied.

¹ Bracketed references are to CM/ECF docket entries, and page references are to CM/ECF pagination.

BACKGROUND

The October 8, 2020 search warrant, signed by Magistrate Judge Roemer for Stuart’s residence located at 1010 Cleveland Drive in Cheektowaga, New York (20-mj-5207), was supported by the Affidavit of FBI Task Force Officer (“TFO”) Michael Hockwater [1].² TFO Hockwater explained that in June of 2019, a computer server hosting “a child pornography bulletin board and website dedicated to the advertisement and distribution of child pornography and the discussion of matters pertinent to the sexual abuse of children” (the “Target Website”), which was located outside of the United States, was seized by a foreign law enforcement agency (“FLA”). *Id.*, ¶15. The Target Website operated on the “Tor network”, which is “designed specifically to facilitate anonymous communication over the Internet”. *Id.*, ¶¶6, 8.

The investigation into Stuart began in August 2019, when a FLA “known to the FBI and with a history of providing reliable, accurate, information in the past, notified the FBI that [it] determined on May 28, 2019 [an IP address later learned to be linked to Stuart and his residence] ‘was used to access online child sexual abuse and exploitation material’ via . . . the [Target Website]”. *Id.*, ¶¶6 n. 1, 24. TFO Hockwater further explained that the:

“FLA is a national law enforcement agency of a country with an established rule of law. There is a long history of U.S. law enforcement sharing criminal investigative information with FLA and FLA sharing criminal investigative information with U.S. law enforcement FLA advised U.S. law that it obtained that information through independent investigation that was lawfully authorized in the FLA’s country pursuant to its national laws. FLA further advised U.S. law enforcement that FLA had not interfered with, accessed, searched or seized any data from any computer in the United States in order to obtain that IP address information. U.S. law enforcement personnel did not participate in the investigative work through which FLA identified the IP address”. *Id.*, ¶26.

² The search warrant application and warrant are docketed in 20-mj-5207. Unless otherwise noted, all citations to the search warrant materials are to the filings in 20-mj-5207.

Stuart initially moved to suppress the evidence seized from the search warrant by arguing, *inter alia*, that the information supplied by the FLA lacked sufficient indicia of reliability. Stuart’s Memorandum in Support of Suppression [27-2] at 1-5. Alternatively, he moved for discovery on that issue. *Id.* at 5. However, several months after that motion was denied (Report, Recommendation and Order [33], adopted, Decision and Order [44]), Stuart claims to have “learned that this case is merely a small part of a vast multi-district, multi-national pornography investigation”, which “revealed that the government’s disclosures to date have been inadequate”. Stuart’s Memorandum in Support [55] at 2. From the government’s disclosures in other similar prosecutions, and additional investigation, Stuart discovered that the search warrant used here was a “batch warrant” (*i.e.*, “nearly identical [warrants] . . . with only the name of the suspect and other individualized information changed”), and that this was a “joint operation, where U.S. law enforcement were working hand in hand with foreign law enforcement agencies to share information, take over targeted websites, and identify visitors to target websites”. Stuart’s Memorandum in Support [55] at 3-4.

Following Stuart’s discovery of this new information, he filed the pending motions.

DISCUSSION

A. Motion to Compel

The government argues that this motion is untimely, as it was filed long after the October 4, 2021 deadline of the Fifth Amended Scheduling Order for filing pretrial motions ([26], ¶1). Government’s Response [66] at 7-8. However, Stuart argues (and the record confirms) that District Judge Vilardo granted him permission to file the motion (Stuart’s Reply

[71] at 1), and there is no indication that the government reserved the right to argue that the motion was untimely, or that Judge Vilardo granted it that right. *See* May 19, 2022 Minute Entry [49] (“AFPD Bagley believes legitimate issues need to be raised, and request[s] time to file a motion to compel. *AUSA Higgins has no position*. Court orders defendant’s motion to be . . . filed by 6/6/2022” (emphasis added)).

Turning to the merits of Stuart’s motion, he initially sought a variety of discovery concerning the FLA’s involvement in the investigation pursuant to Brady v. Maryland, 373 U.S. 83 (1963), as well as Fed. R. Crim. P. (“Rules”) 12(b)(3)(E), 16(a)(1)(E), and 16(a)(1)(F). *See* Stuart’s Memorandum [55] at 3, 10. In response, the government produced several documents pursuant to a Protective Order [73] “as an act of good faith”, but argues that Stuart fails to establish that “any remaining documents are material under Rule 16”. Government’s Response [66] at 2. Its production included:

-- an Intelligence Report from the
stating that on May 28, 2019, an IP address associated with Stuart “was used to access online child sexual abuse and exploitation material” on the Target Website ([75-1] at 1-2);

-- a September 16, 2019 letter from to the FBI stating that the data it provided to the FBI concerning individuals who accessed online child sexual abuse and exploitation material was “lawfully obtained under the Investigatory Powers Act 2016”, and that “[t]he[] warrants . . . were authorised by a Senior Director of and approved by a

”. It further confirmed that “[u]nder these warrants during an independent investigation lawfully authorised under legislation, did not access, search or seize any data from any computer in the United States” (*id.* at 12); and

-- a July 13, 2020 FBI memo providing information to the Buffalo Field Office concerning _____”, targeting “users of multiple Tor hidden service sites”, including the Target Website. The memo attached a draft search warrant affidavit and target IP addresses (id. at 5-10).

Unsatisfied with the government’s good faith production, which he characterizes as only “the tip of the iceberg”, Stuart argues that his investigation revealed that the United States “played a much larger role” in the investigation. Stuart’s Reply [71] at 2. Based on the government’s disclosures, Stuart modified his initial requests ([55] at 10) to seek:

- “• All the [FLAs] and countries involved in all aspects of the investigation.
- What role each FLA had.
- U.S. law enforcement’s full role, including what techniques were utilized and when they were utilized.
- Which U.S. agencies were involved and how.
- All information and documentation related to Project Habitanca in the possession of the prosecution team, as that term is defined by caselaw.
- What technique was used to locate, take down and seize the server.
- What technique was used to de-anonymize the website’s IP address.
- Whether Mr. Stuart had account on the website in question.” Stuart’s Reply [71] at 6.

At the initial oral argument of Stuart’s motion to compel, the government agreed to make additional voluntary disclosures to Stuart. *See* February 15, 2023 Text Order [78].

These included a copy of the sealed Criminal Complaint in United States v. Brandon Kidder, 20-mj-1010, as well as a February 8, 2023 letter [80-1] from AUSA David Rudroff summarizing the background of the investigation from information supplied to him by the FBI and the Department of Justice Child Exploitation and Obscenity Section. The letter claimed that the information it

contained was “neither discoverable, nor relevant to any material issue”, but instead was being provided to “clarify potential misunderstandings regarding the identification of [Stuart’s IP] address”, and to assist “in resolving [Stuart’s] pending motion”. Id. at 1.

In particular, the letter explained that while conducting its own independent investigation into Tor-network based websites dedicated to child pornography, the FBI learned that the “computer server hosting . . . [the Target Website] was operating in _____”, and the FBI provided the IP address of that server to _____ in 2018. Id. at 1. _____ then conducted its “own investigation”, without FBI participation, resulting in the seizure of the server by _____ law enforcement in June 2019. Id. The seized server “hosted multiple hidden services dedicated to child pornography”, and while _____ shared its investigative findings with _____ and FBI, it did not “provide information to the FBI that identified [Stuart’s] IP address”. Id.

Stuart’s IP address was instead provided to the FBI by _____, which was “simultaneously investigating these hidden serves and the users thereof”, but it has “not disclose[d] to the United States the methodology it used to determine that [Stuart’s] IP address accessed material on these hidden services beyond the information and assurances provided in the documents and assurances provided in the documents [Stuart] has received in discovery.” Id. at 2.

The government’s February 8, 2023 letter largely confirms what is contained in two press releases relied upon by Stuart: A January 23, 2000 Interpol press release [71-1] and an undated translated press release from the National Association of Public Prosecutors [89-4]. Stuart acknowledges that the government’s February 8, 2023 letter [80-1] “attempts to answer some of [his] requests with a narrative”, but he contends that the “government has still not provided any documentation or data relative to the requests”, particularly concerning “the

technique or techniques used to deanonymize the IP addresses that purportedly led to the one associated with [him]”. Stuart’s post-argument Memorandum/Brief [80] at 4.

1. Rule 16

Under Rule 16(a)(1)(E)(i) a defendant is entitled to documents and tangible things in the “government’s possession, custody, or control”, so long as “the item is material to preparing the defense”. “A document is material under Rule 16 if its pretrial disclosure will enable a defendant to alter significantly the quantum of proof in his favor.” United States v. Alshahhi, 2022 WL 2239624, *26 (E.D.N.Y. 2022). However, “[c]onclusory allegations are insufficient . . . to establish materiality and the burden is on the defendants to make a *prima facie* showing that the documents sought are material to preparation of the defense.” Id.

Stuart contends that he requires the requested discovery “[t]o properly litigate the pertinent Fourth Amendment issues before the Court, including addressing matters of reliability and veracity”. Stuart’s Memorandum [55] at 7. “While suppression is generally not required when the evidence at issue is obtained by foreign law enforcement officials”, the Second Circuit has recognized two “narrow exceptions” that require suppression “of evidence obtained abroad”. United States v. Lee, 723 F.3d 134, 140, 142 (2d Cir. 2013). First, “where the conduct of foreign officials was so extreme that it would shock the judicial conscience”, and second, “where the nature of the cooperation implicated constitutional restrictions”. Id. at 142. “[U]nder the ‘constitutional restrictions’ exception, constitutional requirements may attach in two situations: (1) where the conduct of foreign law enforcement officials rendered them agents, or virtual agents, of United States law enforcement officials; or (2) where the cooperation between the United States and foreign law enforcement agencies is designed to evade constitutional

requirements applicable to American officials.” United States v. Getto, 729 F.3d 221, 230 (2d Cir. 2013).³

Stuart seeks discovery to establish the applicability of these exceptions. In support of his contention that the search warrant for his residence was the result of a “joint operation” between the FBI and an FLA, Stuart argues that the Criminal Complaint Affidavit in United States v. Clark, 2:21-MJ-00147 (W.D. Wash.), which also arose from _____, “described the investigation as ‘collaborative’ between U.S. and foreign law enforcement”. Stuart’s Memorandum [55] at 4. This lone statement - from a different case - falls short of establishing a *prima facie* showing that _____ acted as an agent (or virtual agent) of the United States in obtaining Stuart’s IP address or that there was cooperation between the two to evade United States constitutional protections. Despite characterizing it as a “collaborative investigation”, the Affidavit in Clark ([55-3], ¶¶5-8) offers nothing to suggest that the collaboration extended beyond what occurred here - _____ providing the FBI with an IP address that accessed the targeted website.

The government’s disclosures demonstrate that there was some information sharing between the FBI and _____ that led to the seizure of the host server. However, even if this rose to the level of cooperation that implicated constitutional restrictions (which it does not),

³ Stuart repeatedly points to this being a “joint venture”. *See, e.g.*, Memorandum in Support [55] at 8. Some Circuits have recognized a joint venture exception, where the “participation of federal agents [may] be so substantial [in a foreign investigation] so as to convert the search into a joint venture”. United States v. Behety, 32 F.3d 503, 511 (11th Cir. 1994). However, as the government notes ([92] at 15), the Second Circuit has “repeatedly declined to adopt the joint venture doctrine in the context of the Fourth Amendment”. Getto, 729 F.3d at 233. Instead, “the longstanding principles of ‘virtual agency’ and intentional constitutional evasion . . . [are] the applicable analytic rubric to determine whether cooperation with foreign law enforcement officials may implicate constitutional restrictions”. *Id.* Therefore, I have treated Stuart’s “joint venture” references as relying on the virtual agency exception, and this appears to align with his own use of that term. *See* Memorandum in Support [55] at 8 (“whether the FLAs acted with U.S. agents, at the behest of U.S. agents, or as agents for their American counterparts, such that there was a ‘joint venture’”).

did not provide the FBI with Stuart's IP address. Nor has Stuart established a reasonable expectation of privacy in the content of the Target Website's host server. *See United States v. Werdene*, 188 F. Supp. 3d 431, 445 (E.D. Pa. 2016), *aff'd on other grounds*, 883 F.3d 204 (3d Cir. 2018) ("[e]ven if Werdene maintained a subjective expectation that his IP address would remain private through his use of Tor, that expectation is not 'one that society is prepared to recognize as 'reasonable'"); *United States v. Scanlon*, 2017 WL 3974031, *11 (D. Vt. 2017), *aff'd*, 774 F. App'x 43 (2d Cir. 2019) ("any expectation by a Playpen user that his or her identity could not and would not be revealed while accessing child pornography on a publicly available website is not one society would deem reasonable").

The remainder of Stuart's motion focuses primarily on obtaining the method used by [redacted] to identify his IP address. He contends that without this information, "there is simply no way to know if the IP address that the second FLA said visited the website *actually visited* the website. The mystery technique might have gotten it wrong". Stuart's Memorandum/Brief [80] at 3 (emphasis in original). In short, he contends that without this information, the government "cannot assure the court that it does not shock the conscience". *Id.* at 4.

First, Stuart attempts to cast doubt on [redacted] representation that no computers in the United States were accessed by [redacted] ([75-1] at 12) by pointing to the expert Declaration of Steven Murdoch [55-4] submitted in *United States v. Sanders*, 20-CR-00143 (E.D. Va. 2021), which "suggests that the specific IP address could not have been identified without running a NIT [Network Investigation Technique]", malware "designed to gain access to . . . a computer without the owner's consent". Stuart's Memorandum [55] at 8. *See also United*

States v. Bateman, 2021 WL 3055014, *3 (D. Mass. 2021) (NITs “amount to government installation of malware on a user’s computer”).

However, as the court explained in United States v. Kiejzo, 2022 WL 1078214, *6 (D. Mass. 2022), “Professor Murdoch’s affidavit suggests one must ‘control’ a subject website on the Tor network to implement an NIT. (. . . at ¶28). Thus, to the extent an NIT was used in this case, Professor Murdoch’s affidavit suggests that it was implemented by the Seizing FLA, not the Notifying FLA.” The same holds true here: nothing offered by Stuart suggests that controlled the Target Website, thereby enabling it to have utilized a NIT to retrieve Stuart’s IP address. *See Kiejzo*, 2023 WL 2601577, *8 (NITs “unmask Tor users by tracking them contemporaneously with their access of servers”).⁴

Stuart further argues that the potential use of the error-prone traffic analysis technique “would undermine the strength and reliability of the tip such that no magistrate, had he or she been aware that this technique was used to obtain the IP address, would find there was probable cause”. Stuart’s Memorandum [55] at 9. However, similar arguments have been rejected as “speculative”. Kiejzo, 2022 WL 1078214, *6.

Finally, Stuart cites United States v. Mitrovich, 458 F. Supp. 3d 961 (N.D. Ill. 2020) (Reply Memorandum [75] at 5-6), which involved a similar Tor hosted child pornography website that was investigated by an FLA and resulted in the FLA’s production of the defendant’s IP address to the FBI, as an address that accessed the website. Unlike here, the FLA in

⁴ As the government also notes (Response [66] at 12), not only is the applicability of Professor Murdoch’s Declaration to this case speculative, but Murdoch identifies at least one other way to de-anonymize Tor users without accessing their computers. *See* Murdoch Declaration [55-4], ¶23 (“there are only two techniques for identifying the IP address of a user using Tor Browser properly: traffic-analysis (which can generate errors) or a [NIT] (which interferes with a user’s computer)”). Likewise, the court in Sanders noted that the case agent had submitted a declaration identifying “possible publicly known methods of de-anonymizing Tor users without interfering with the user’s computer”. *See* Sealed Memorandum Opinion [66-1] at 14 (document pagination), n. 11.

Mitrovich continued to operate the website in an undercover capacity following its seizure. Id. at 963. While doing so, the FLA used a hyperlink posted on the website to capture the IP address of the defendant when he opened the link. Id. The defendant argued that ““because of the way the Tor Network and Tor Browser operates””, the FLA must have deployed malware to identify his IP address. Id. at 966. Coupled with the FBI’s use of malware to discover IP addresses in other investigations, the court concluded that the defendant had “made ‘at least a *prima facie* showing’ that malware was used to obtain his IP address”. Id. at 967. The court explained that the motion could not “be denied based on the Government’s assertion - which rests on second-hand information from [the FLA] - that malware was not used and therefore no Fourth Amendment search occurred”. Id.

Not only is Mitrovich not controlling, but it is also distinguishable from the circumstances of this case. Here, the government has produced a letter directly from stating that no computer in the United States was accessed in order to obtain Stuart’s IP address. [75-1] at 12. While Stuart seeks the precise methodology used to access his IP address in order to assure that it did not “shock the conscience”, there is nothing to suggest that

techniques would do so, particularly since lawfully obtained, under the laws of ([75-1] at 12), the IP addresses that accessed child pornography on the Target Website. *See Lee*, 723 F.3d at 142 (the “narrow” exceptions that can bar evidence gathered abroad, “do not suggest, much less require, that the government or the District Court had a duty to review the legality, under [the foreign] law, of the applications for surveillance authority considered by [the foreign] courts. Indeed, even if [foreign] law enforcement officers somehow operated improperly under [foreign] law in obtaining [the evidence] . . . nothing in this

record shows that they operated in a manner that would implicate either of the limited exceptions”).

In any event, “the Government has no obligation to turn over materials that it does not have and cannot obtain through good faith, diligent efforts”. United States v. Mitrovich, 547 F.Supp.3d at 833, 838 (N.D.Ill. 2021). Therefore, I could not grant Stuart the relief he seeks, *i.e.*, to compel production of the methodology for how obtain Stuart’s IP address. *See Kiejzo*, 2022 WL 1078214, *6 (“perhaps fatal to the defendant’s request for this information, the government has represented that it does not have information on how FLA’s uncovered the defendant’s IP address”); United States v. Hatcher, 622 F.2d 1083, 1088 (2d Cir. 1980) (“[c]learly the government cannot be required to produce that which it does not control and never possessed or inspected”). At most, I could only direct the government to seek to obtain this information from (see Mitrovich, 547 F.Supp.3d at 838), but a sufficient showing for that relief has also not been established.

Some courts have characterized arguments similar to those raised by Stuart as built on a “stack of hypotheticals”. Bateman, 2021 WL 3055014 at *3-4. However, in Kiejzo, another prosecution that appears to arise from this or a related investigation, the government took the position, in responding to a Franks motion, “that it is not possible for IP addresses to be retroactively extracted from a seized Tor server”, which the court found “at least supports, even if it does not confirm, the defendant’s theory that his IP address was identified by something like an NIT - which is likely a search under the Constitution”. 2023 WL 2601577, *7.

Nevertheless, the court concluded that “the possible use of an NIT by an FLA, consistent with its own laws, would [not] shock the conscience”. *Id.* at *9; Kiejzo, 2022 WL 1078214, *5 (“[t]o bring a foreign law enforcement search within the ambit of the Fourth

Amendment, it is not enough that the search violated United States law; it must have shocked the judicial conscience ‘Circumstances that will shock the conscience are limited to conduct that ‘not only violates U.S. notions of due process, but also violates fundamental international norms of decency’”). *See also* Getto, 729 F.3d 221, 229 (2d Cir. 2013) (“‘[t]he shocks the judicial conscience standard is meant to protect against conduct that violates fundamental international norms of decency’”). For that reason as well, Stuart’s motion is denied.

2. Brady

“Brady material . . . includes all evidence which may be favorable to the defendant and material to the issue of guilt or punishment.” United States v. Weishan, 2016 WL 75166, *4 (W.D.N.Y. 2016). Stuart appears to seek the requested discovery to establish that he was misidentified as an individual who accessed the website (*see, e.g.*, Memorandum/Brief [80] at 3 (“there is simply no way to know if the IP address that the second FLA said visited the website *actually visited* the website. The mystery technique might have gotten it wrong” (emphasis in original))).

However, he offers nothing other than speculation that the government is withholding Brady material in its possession. *See* United States v. Upton, 856 F. Supp. 727, 746 (E.D.N.Y. 1994) (“[a]s a matter of law, mere speculation by a defendant that the government has not fulfilled its obligations under Brady v. Maryland . . . is not enough to establish that the government has, in fact, failed to honor its discovery obligations”). Without more, I have no reason to question the government’s representations concerning its compliance with its Brady obligations. *See* Government’s Response [66] at 13 (“the government understands its continuing

obligations under Brady” and “[i]f, in the future, [it] becomes aware of evidence subject to disclosure under Brady, [it] will produce that information to the defense”).

Moreover, “[t]he Government’s Brady obligations extend only to materials within prosecutors’ possession, custody or control”, United States v. Collins, 409 F. Supp. 3d 228, 239 (S.D.N.Y. 2019), and the government has stated that [redacted] has “not disclose[d] to the United States the methodology it used to determine that [Stuart’s] IP address accessed material on these hidden services beyond the information and assurances provided in the documents and assurances provided in the documents [Stuart] has received in discovery”. February 8, 2023 letter [80-1] at 2. Nor does Brady “require the government to search for exculpatory material not within its possession or control”. United States v. Raniere, 384 F. Supp. 3d 282, 325 (E.D.N.Y. 2019).

Courts have held that where “the United States Attorney’s Office conducts a ‘joint investigation’ with another state or federal agency . . . the prosecutor’s duty extends to reviewing the materials in the possession of that other agency for Brady” (*id.*), but even if that principle applied to joint investigations with a FLA, there is no evidence that this was a joint investigation between [redacted] and FBI. Therefore, this portion of the motion is also denied.

B. Renewed Motion for Suppression and for a Franks Hearing

1. Timeliness

The government argues that Stuart’s motion is untimely, as it was filed nearly 18 months after the October 4, 2021 pretrial motion deadline of the Fifth Amended Scheduling Order ([26], ¶1) and Stuart has not shown good cause to overcome its untimeliness. Government’s Response [92] at 6-8.

Under Rule 12(c)(3), “[i]f a party does not meet the deadline for [filing certain pretrial motions, including motions to suppress], the motion is untimely. But a court may consider the defense, objection, or request if the party shows good cause”. As the government notes, courts have recognized that “‘counsel’s failure to conduct proper pretrial investigation does not establish good cause for a defendant’s failure to raise an argument covered by Rule 12(b)(3) in a timely fashion’”. Government’s Response [92] at 7 (*quoting United States v. Gerace*, 2022 WL 19003139, *4 (W.D.N.Y. 2022), adopted, 2023 WL 1775754 (W.D.N.Y. 2023)).

There is no indication that Judge Vilardo gave Stuart permission to file any motion other than his motion to compel [55]. *See* May 19, 2022 Minute Entry [49]. Although some of the discovery that Stuart relies upon for this motion was only produced in response to his recent motion to compel, it is difficult to understand why Stuart could not have earlier investigated the full scope of the investigation that led to the search warrant and timely sought to obtain that discovery and the other relief he now seeks. As the government notes, Stuart was “capable of undertaking the same internet searches he undertook in preparing this motion and finding the public records that he cites”, including the Interpol press release [71-1] published in January 2020. Government’s Response [92] at 8.

Stuart argues that he only later came to learn that “similar, if not identical, cases have sprung up throughout the country”. Stuart’s Memorandum in Support [55] at 2. However, TFO Hockwater’s Affidavit stated that the Target Website had over 230,000 members as of June 2019 ([1], ¶17), making it “strange if the notifying FLA . . . only identified a single American user”. *Kiejzo*, 2023 WL 2601577, *8.

In any event, it is unnecessary for me to resolve the government's timeliness arguments, since for the reasons that follow, I conclude that Stuart is not entitled to a Franks hearing or to suppress the evidence located as a result of the search warrant for his residence.

2. Franks hearing

"The Franks standard is a high one". Rivera v. United States, 928 F.2d 592, 604 (2d Cir. 1991). "To be entitled to a Franks hearing, a defendant must make a substantial preliminary showing that: (1) the claimed inaccuracies or omissions are the result of the affiant's deliberate falsehood or reckless disregard for the truth; and (2) the alleged falsehoods or omissions were necessary to the judge's probable cause finding." United States v. Salameh, 152 F.3d 88, 113 (2d Cir. 1998).

Since affidavits supporting search warrants are entitled to "a presumption of validity", in order to "mandate an evidentiary hearing, the challenger's attack must be more than conclusory and must be supported by more than a mere desire to cross-examine." Franks, 438 U.S. at 171. Therefore, "[t]here must be allegations of deliberate falsehood or of reckless disregard for the truth, and those allegations must be accompanied by an offer of proof." Id.

Stuart raises several arguments in support of his entitlement to a Franks hearing. First, he argues that TFO Hockwater's Affidavit "omitted the crucial fact that the homepage of the [Target] [W]ebsite did not display any child sexual abuse material", and instead required an individual to "navigate past the homepage of the website" in order to access child sexual abuse material. Stuart's Memorandum [89] at 8. He contends that "[h]ad Hockwater been truthful about the tip and stated that U.S. law enforcement had received information only that the IP address was used to visit a website where no child pornography was visible or available on the

homepage, the magistrate could not have found sufficient probable cause to issue the warrant”.
Id. at 9.

Nothing before me could lead me to conclude that TFO Hockwater deliberately omitted this information. The discovery produced confirms that his Affidavit merely parroted what [redacted] had relayed - that a particular IP address “was used to access online child sexual abuse and exploitation material” on the Target Website. [75-1] at 1-2. Moreover, even if TFO Hockwater had deliberately omitted the fact that the homepage of the Target Website did not contain child pornography, the inclusion of this information would not have undermined the existence of probable cause. *See United States v. Rajaratnam*, 719 F.3d 139, 146 (2d Cir. 2013) (“[t]he ultimate inquiry is whether, after . . . correcting material omissions, there remains a residue of independent and lawful information sufficient to support a finding of probable cause”). Elsewhere TFO Hockwater explained that since it was a “hidden service website” that “required numerous affirmative steps” to locate and access, it was “extremely unlikely” that the user of the IP address “could simply stumble upon [the] [Target Website] without understanding its purpose and content”. [1], ¶¶28, 30. Therefore, he believed that “any user who accessed” the Target Website did so “with intent to view child pornography, or attempted to do so”. Id., ¶31.

The suspected crimes for which the warrant authorized a search (18 U.S.C. §§2252A(a)(5)(B) and 2252A(b)(2)) do not require the user to actually view child pornography on the Target Website. *See United States v. Tagg*, 886 F.3d 579, 587, 588 (6th Cir. 2018) (“[t]he access-with-intent offense [of 18 U.S.C. §2252A(a)(5)(B)] is complete the moment that the elements of access and intent coincide. Thus, even if the person never viewed illegal child pornography, knowingly accessing a child-pornography website with the intent to view illegal materials is itself a criminal act. It follows from this language that probable cause to search . . .

would exist even if he was ‘curiosity shopping’ for child porn . . . but never actually viewed an illegal image”); 2252A(b)(2) (criminalizing “[w]however . . . *attempts* . . . to violate [2252A(a)(5)]” (emphasis added)). Therefore, whether or not images of child pornography were located on the homepage of the Target Website, it was the act of accessing the site alone that created probable cause to search the residence.

Next, Stuart argues that TFO Hockwater “omitted from the affidavit the fact that there was not just one FLA involved in the investigation of the website, but two - from entirely different countries”. Stuart’s Memorandum [89] at 10. While TFO Hockwater “made a number of claims in the affidavit about the reliability of the FLA, those statements applied *only* to the FLA that provided the tip to U.S. law enforcement. There are no facts in the affidavit that address or establish the reliability . . . of . . . the FLA that seized the server”. *Id.* at 11 (emphasis in original). According to Stuart, “[w]ithout assurances in the affidavit about the reliability and trustworthiness” of “and the legality of its action, no Magistrate could find there was probable cause”. *Id.*

In response, the government argues that since Stuart has “failed to establish - or even allege - that TFO Hockwater was aware of the involvement of a second FLA at the time of the warrant application”, he cannot “establish that the omission of this information . . . was intentional and omitted to deceive the issuing Magistrate”. Government’s Response [92] at 13. I agree.

Moreover, even if this was a deliberate omission, it was immaterial. Had TFO Hockwater’s Affidavit included information concerning the preceding seizure of the Target Website’s server by , without any assurances as to its reliability as a FLA, it is not clear how that would undermine the existence of probable cause, particularly since there is nothing

that indicates that _____ provided Stuart’s IP address, or any other information in TFO Hockwater’s Affidavit, to the United States. *See Kiejzo*, 2023 WL 2601577, *6 (“a credibility determination is only necessary if the FLA provided the United States with information. There is no indication in the affidavit that the seizing FLA provided any information to the United States”).

Finally, relying on the Interpol [71-1] and National Association of Public Prosecutors [89-4] press releases, Stuart argues that TFO Hockwater “withheld information that would have shown that 1) U.S. law enforcement was engaged in a ‘joint venture’ with the FLAs and 2) the FLAs engaged in conduct that would shock the judicial conscience such that the FLAs’ actions would be subject to the exclusionary rule”. Stuart Memorandum [89] at 12.

The press releases that Stuart relies upon largely correspond to the investigative summary provided by AUSA Rudroff to Stuart in his February 8, 2023 letter [80-1]. As the letter confirms, the FBI, while conducting its own independent investigation into Tor-network based websites dedicated to child pornography, learned that the “computer server hosting . . . [the Target Website] was operating in _____”, and the FBI provided the IP address of that server to _____ law enforcement in 2018. *Id.* at 1. *See also* National Association of Public Prosecutors’ press release [89-4] at 2-3. The February 8, 2023 letter also stated that authorities provided evidence obtained through its investigation and from the seizure of that server to _____ and other international law enforcement agencies, including the FBI” [80-1]. *See* National Association of Public Prosecutors’ press release [89-4] at 5.

Even if TFO Hockwater deliberately omitted this additional information to mislead Judge Roemer, its inclusion would not alter the existence of probable cause for the search warrant. “Because there is no evidence that _____ the seizing FLA[,] provided

information to the United States”, the omission of this information is not material. Kiejzo, 2023 WL 2601577, *6.

The primary source of probable cause for the search warrant for Stuart’s residence was tip that “on May 28, 2019, [an IP address later determined to be associated Stuart], ‘was used to access online child sexual abuse and exploitation material’ via . . . the [Target Website]”. [1], ¶24. However, even if that information was obtained by through its use of a NIT as Stuart alleges, there is nothing to suggest that TFO Hockwater was aware of this. Moreover, “[s]o long as the search came from a credible partner, was not done in concert with the United States, and does not shock the conscience, the fruits of searches of Americans by FLAs may be used to support an application for a warrant. That there was likely a search is not, in and of itself, material”. Kiejzo, 2023 WL 2601577, *7. Therefore, I recommend that Stuart’s motion for a Franks hearing be denied.

3. Suppression

Stuart moves to re-open his previously denied motion to suppress. That motion was based in part on the alleged lack of reliability of the information supplied by the FLA. In denying that motion, Judge Vilardo explained:

“The Third Circuit addressed this issue in [United States v. Benoit, 730 F.3d 280 (3d Cir. 2013)] and found that ‘a tip from one federal law enforcement agency to another implies a degree of expertise and a shared purpose of stopping illegal activity.’ Benoit, 730 F.3d at 285. Therefore, ‘given that the source . . . was not only known to the DEA, but was also a repeat-player in the United States’ efforts at drug-trafficking prevention,’ the Third Circuit held that “the information had sufficient indicia of reliability.” Id. This Court agrees with that holding, and because the information here had at least the same indicia of reliability, it reaches the same result.

Hockwater’s affidavit advised that the FLA is the national law enforcement agency of a country with an established rule of law. . . . In fact, Hockwater said that the

FBI knew the identity of the FLA and that the FLA had provided ‘reliable, accurate information in the past.’ . . . And Hockwater noted that this particular FLA and law enforcement agencies in the United States had a ‘long history’ of exchanging criminal investigative information, including information concerning the investigation of crimes against children That was enough to credit the reliability of the FLA and the information it provided, and Judge Roemer did not err in so finding.

Indeed, neither the name of the country nor the name of the specific law enforcement agency would have added much under the circumstances here. What was provided, and what was and is critical to determining reliability, was the FLA’s track record of sharing and providing reliable and accurate information.” April 7, 2022 Decision and Order [44] at 7-8.⁵

Stuart argues that the new information that he has gathered “completely changes the landscape”. Stuart’s Memorandum [89] at 18. He points to the fact that he has learned that “used an unknown technique to deanonymize the IP addresses”, which left TFO Hockwater unable to “make any assurance as to the reliability of the method used to produce the IP address in this case”. Stuart’s Memorandum [89] at 18-19. He next contends that TFO Hockwater failed to specify whether the FLA’s purported previous reliability had anything to do with the subject area at issue in this case. *Id.* at 19. Finally, he suggests that “we now know” that the FLA’s tip that the IP address “was used to access online child sexual abuse and exploitation material” was not accurate and reliable information, insofar as we now know that the user may have accessed the Target Website’s home page, but not the underlying child pornography. *Id.*

⁵ Kiejzo supports Judge Vilardo’s earlier decision: “The Court is wary of a practice by which the government might take a ‘see no evil’ approach to working with FLAs, even reliable ones, because it is difficult to access this information within the confines of the Fourth Amendment. However, the Court is also cognizant of the international and anonymous nature of these crimes. Ultimately, the Court may only overturn a magistrate judge’s evaluation if there is ‘no substantial basis for concluding that probable cause existed.’ Under that deferential standard, the magistrate judge did not err in crediting the tip given the notifying FLA came from a country with a rule of law, the investigation was conducted according to the country’s laws, and past tips had resulted in arrests, seizures, and rescues.” 2023 WL 2601577, *3.

Several of these arguments could have raised at the time of Stuart's initial motion. In any event, none of these additional arguments or information undermine the indicia of reliability that Judge Vilardo previously concluded existed from the information presented in the four corners of TFO Hockwater's Affidavit. "[A]s long as the applicant for the warrant accurately represents the information provided by an informant, probable cause is not defeated because the informant erred, or even lied, in his description of events." United States v. Smith, 9 F.3d 1007, 1014 (2d Cir. 1993).

Alternatively, the government argues that even if "the newly discovered information does somehow vitiate probable cause", the evidence obtained from the search warrant would still be admissible under the good faith exception of United States v. Leon, 468 U.S. 897 (1984). *See* Government's Response [92] at 17. "When police act under a warrant that is invalid for lack of probable cause, the exclusionary rule does not apply if the police acted in objectively reasonable reliance on the subsequently invalidated search warrant." Herring v. United States, 555 U.S. 135, 142 (2009).

"The burden is on the government to demonstrate the objective reasonableness of the officers' good faith reliance on an invalidated warrant." United States v. Clark, 638 F.3d 89, 100 (2d Cir. 2011). There are "four circumstances where an exception to the exclusionary rule would not apply: (1) where the issuing magistrate has been knowingly misled; (2) where the issuing magistrate wholly abandoned his or her judicial role; (3) where the application is so lacking in indicia of probable cause as to render reliance upon it unreasonable; and (4) where the warrant is so facially deficient that reliance upon it is unreasonable." Id.

TFO Hockwater's 44-page search warrant Affidavit was not so lacking in probable cause that reliance upon it would have been objectively unreasonable. Nor is there any

indication that Judge Roemer was *knowingly* misled by TFO Hockwater or that Judge Roemer abandoned his judicial role in any way. “[W]hile certain details were excluded from the affidavit - such as the fact that the Notifying FLA was not the same as the Seizing FLA - [the] Agent . . . expressly averred that []he included only facts []he believed were necessary to establish probable cause.” Kiejzo, 2022 WL 1078214, *5. *See* Hockwater Affidavit [1], ¶3 (“I have not included each and every fact known to me concerning this investigation. I have set forth only the facts that I believe are necessary to establish probable cause”).

Therefore, even if I had determined that the search warrant was not supported by probable cause, I would nevertheless conclude that the good faith exception applies, and accordingly recommend that Stuart’s renewed motion for suppression be denied.

C. Motion to Modify the Protective Order

In connection with the materials that the government voluntarily produced following Stuart’s motion to compel [55], it moved for the entry of a Protective Order, because “[s]ome of the discovery that [it] has provided or intends to provide contains information that could jeopardize ongoing investigations, including the names of child pornography websites on the dark web and details regarding information sharing between U.S. and foreign law enforcement.” [72] at 1. The government argued that “[t]his information has been used to generate investigative leads that have been distributed to law enforcement around the country”, but “[n]ot all of these leads have been acted on by law enforcement.” Id. Stuart had no objection to the entry of the Protective Order, but reserved his right to move for relief from the order if necessary. Id. at 2. Therefore, I granted the unopposed motion and entered the Protective Order the same day [73].

Stuart now moves to modify the Proctive Order, alleging that “the reasons the government offered for the Protective Order are not compelling, and the limitations imposed by the Order are hampering [his] preparations for trial and continued motion practice”. Stuart’s Memorandum [85] at 2. He claims that “[p]ublic documents discovered by the defense have already publicized much, if not all, of the information that the government seeks to protect - including the name of one of the websites”. Id. at 4.

Rule 16(d)(1), governing protective orders, provides that “[a]t any time, the court may, for good cause, deny, restrict, or defer discovery or inspection, or grant other appropriate relief.” “The Second Circuit has not directly addressed the meaning of ‘good cause’ in the context of modification of a protective order in a criminal case”, “[b]ut district courts within this Circuit have generally applied the same standard that exists in civil cases.” United States v. Ngono, 2021 WL 2850626, *1 (S.D.N.Y. 2021). Under that standard, “a strong presumption against modifying a protective order applies if the parties to the protective order reasonably relied on it.” Id. The “presumption can be overcome only if there is a showing of ‘improvidence in the grant of the order or some extraordinary circumstance or compelling need.” Id. at *3.

“Courts consider several factors in determining whether a protective order reasonably invited reliance: (1) the order’s scope; (2) the order’s express language; (3) the level of inquiry the court gave prior to granting the order; (4) the nature of the reliance; and (5) the type of materials that the party seeking modification is attempting to access.” Id. at *2. Ultimately, however, “[t]hese factors are non-exhaustive, and whether to modify a protective order is entrusted to the discretion of the District Court”. Id.

Although Stuart points out that my review of the unopposed Protective Order was limited, and that the Protective Order expressly contemplated his ability to move for

modification ([72] at 2 (Stuart “reserves the right to move for relief from the order”)), the balance of the factors, and other considerations, support application of the presumption against modification, and Stuart fails to demonstrate any extraordinary or compelling need to overcome that presumption. As the government notes, it “relied on the protective order when it elected to provide discovery that contained sensitive investigative information without a corresponding discovery obligation”. Government’s Response [87] at 7 n. 1.

The Protective Order is also limited in scope. While Stuart claims that he is unable to consult with experts, the government points out that the Protective Order does not prohibit him from doing so. Government’s Response [87] at 7. In fact, the Protective Order expressly permits discovery materials designated “sensitive” to be shared with his experts and other members of the defense team, so long as those individuals agree to be bound by the terms of the Protective Order.

Stuart also seeks to share discovery with “other defense counsel, all of whom have similar cases pending in federal courts throughout the county”. Stuart’s Reply [88] at 3. In support of modifying the Protective Order to allow for this collaboration, Stuart relies upon United States v. Michaud (CR15-05351) (W.D. Wash), where the court modified its protective order in a similar action to permit the defendant to share sensitive discovery with other defense teams representing clients that had been charged with accessing the same website. *See* Revised Discovery Protective Order, CR15-05351 (W.D. Wash), [62], ¶4. However, the court in Michaud offered no explanation for its decision to modify the protective order, and is not controlling authority.

While it is understandable that Stuart’s counsel may want to collaborate with attorneys defending similar cases, this can be accomplished short of producing the discovery in

this action to others. For instance, the Protective Order limits who may *possess* the sensitive discovery, but does not expressly prohibit Stuart’s attorney from *discussing* it with others. *See* Protective Order [73], ¶2 (“[p]ossession of *copies* of the discovery materials . . . is limited to the attorneys of record” (emphasis added)); ¶3 (“the defense team may not provide *copies* of . . . discovery materials to the Defendant or any other person” (emphasis added)).

If production of the discovery to a specific attorney or group of attorneys becomes necessary to aid in Stuart’s defense, Stuart may renew his motion or, as the government notes, “the [P]rotective [O]rder does not prohibit dissemination of ‘sensitive’ materials to his attorneys”, thereby leaving him “free to retain any non-conflicted attorney he would like, and to share ‘sensitive’ discovery with them.” Government’s Response [87] at 8.

While Stuart points to the presumption in favor of public disclosure (Stuart’s Memorandum [85] at 3) and that the evidence in this case was secured four years ago (Reply Memorandum [88] at 3), “courts have repeatedly recognized that materials . . . can be kept from the public if their dissemination might adversely affect law enforcement interests”, including revealing ongoing criminal investigations and law-enforcement methods. United States v. Smith, 985 F. Supp. 2d 506, 531 (S.D.N.Y. 2013). Therefore, I have no reason to question the government’s representations both in its motion for a protective order [72] and opposition to this motion ([87] at 5) concerning the legitimate law enforcement objectives for limiting disclosure of these materials.

Stuart suggests that the government’s claimed need to protect information in this case from disclosure is inconsistent with its actions, noting that identify of that the Target Website that he allegedly accessed - information the government claims should not be publicly disseminated - was identified in the Department of Justice’s own public filing. *See* Stuart’s Reply

[85] at 4. However, the government counters that this lone reference was buried 30 pages into a DOJ submission to Congress, and that the Target Website remains “not widely known”.

Government’s Response [87] at 5. More importantly, it notes that the “scope and nature of the government’s investigation into that website and its users is not widely known or public”. Id.

Absent some evidence that the public’s knowledge of the Target Website and the related investigation is greater than the government alleges, I am not inclined to lift or modify the Protective Order at this time. Therefore, the motion is denied, without prejudice.

CONCLUSION

For these reasons, Stuart’s motions to compel [55] and vacate [85] are denied, and I also recommend that his motion for a Franks hearing and to suppress [89] be denied. Unless otherwise ordered by District Judge Vilardo, any objections to this Report, Recommendation and Order must be filed with the clerk of this court by June 5, 2023. Any requests for extension of this deadline must be made to District Judge Vilardo. A party who “fails to object timely . . . waives any right to further judicial review of [this] decision”. Wesolek v. Canadair Ltd., 838 F. 2d 55, 58 (2d Cir. 1988); Thomas v. Arn, 474 U.S. 140, 155 (1985).

Moreover, the district judge will ordinarily refuse to consider *de novo* arguments, case law and/or evidentiary material which could have been, but were not, presented to the magistrate judge in the first instance. Patterson-Leitch Co. v. Massachusetts Municipal Wholesale Electric Co., 840 F. 2d 985, 990-91 (1st Cir. 1988).

The parties are reminded that, pursuant to Rule 59(c)(2) of this Court’s Local Rules of Criminal Procedure, “[w]ritten objections . . . shall specifically identify the portions of the proposed findings and recommendations to which objection is made and the basis for each

objection, and shall be supported by legal authority”, and pursuant to Local Rule 59(c)(3), the objections must include “a written statement either certifying that the objections do not raise new legal/factual arguments, or identifying the new arguments and explaining why they were not raised to the Magistrate Judge”. Failure to comply with these provisions may result in the district judge’s refusal to consider the objection.

Dated: May 22, 2023

/s/Jeremiah J. McCarthy
JEREMIAH J. MCCARTHY
United States Magistrate Judge